УДК 621.391(075.8)

НОРМЕННОЕ ДЕКОДИРОВАНИЕ ОШИБОК ПОСРЕДСТВОМ ИХ МОДИФИКАЦИИ

В.А. ЛИПНИЦКИЙ, АЛЬ-ХАЙДАР Е.К.

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, Минск 220013, Беларусь

Поступила в редакцию 7 октября 2009

Предложен модифицированный норменный метод коррекции ошибок в двоичных БЧХ-кодах произвольной длины и произвольным кодовым расстоянием. Суть метода в отображении ошибок с не равной нулю первой компонентой синдрома в ошибки того же веса, но с нулевой первой компонентой синдрома.

Ключевые слова: линейный помехоустойчивый код, двоичный код, БЧХ-код, синдром ошибок, теория норм синдромов, норменный метод коррекции ошибок.

Введение

Жизнь в условиях современной информационной эпохи предъявляет жёсткие и противоречивые требования к передаче, обработке и хранению информации. Подавляющая часть телекоммуникационных систем (ТКС) функционирует с применением помехоустойчивых кодов. Теория и практика помехоустойчивого кодирования существует немногим более полувека, но переживает период постоянного и бурного развития, что отражается, в частности, в росте количества монографий и учебников, посвящённых данной теме (см., к примеру, [1 - 3]).

Теория норм синдромов [4, 5] предоставляет эффективный перестановочный норменный метод коррекции ошибок линейными кодами из семейства БЧХ-кодов. Этот метод обходится без решения уравнений в полях Галуа, на порядок уменьшает влияние проблемы селектора, даёт конструктивный подход к решению проблемы избыточности применяемых кодов, допускает техническую реализацию декодеров на однородных структурах.

Увеличение длин кодов и веса корректируемых ошибок замедляет работу и норменных методов коррекции ошибок, на новом витке актуализируя проблему селектора. В настоящее время идёт проработка различных подходов к дальнейшему сокращению объёма селектируемой совокупности ошибок. Оригинален метод выхода к ошибкам большей кратности [6]. В данной работе предлагается прямой подход, позволяющий сократить объём селектируемой совокупности $\Gamma-$орбит. Суть его в преобразовании искомого вектора-ошибки в класс векторов-ошибок с узко очерченным спектром значений норм, а именно, в класс векторов-ошибок того же веса, но с первой компонентой синдрома $s_1 = 0.$

Суть норменного метода

Норменный метод применяется к циклическим кодам – инвариантным относительно группы $\Gamma = \{\sigma, \sigma^2, ..., \sigma^n = id\}$ циклических сдвигов координат векторов, где $n-$ длина кода и для любого вектора $\bar{e} = (e_1, e_2, ..., e_n)$ $\sigma(\bar{e}) = (e_n, e_1, e_2, ..., e_{n-1}).$ Метод базируется на разбиении векторов-ошибок декодируемой совокупности K на $\Gamma-$орбиты – непересекающиеся между собой классы векторов-ошибок, переходящих друг в друга под

действием автоморфизмов группы Γ. $\Gamma-$орбиты содержат, как правило, по n различных векторов-ошибок, синдромы которых имеют чётко очерченный спектр.

Ряд циклических кодов позволяют находить нормы синдромов – инварианты $\Gamma-$орбит, вычисляемые через синдромы векторов-ошибок, не меняющиеся под действием σ на эти векторы, попарно различные для всех орбит декодируемой совокупности. При названных обстоятельствах суть норменного метода становится очевидной. При получении телекоммуникационной системой (ТКС) очередного вектора-сообщения $\bar{x}$ с ненулевым синдромом ошибок $S(\bar{x})$ вычисляется его норма синдромов $\overline{N} = \overline{N}(S(\bar{x}))$. Норма $\overline{N}$ однозначно указывает какой конкретно $\Gamma-$орбите J декодируемой совокупности K принадлежит вектор-ошибка $\bar{e}$ в сообщении $\bar{x}$. Зная какой-нибудь из векторов $\bar{e}_J$ $\Gamma-$орбиты J, сравнением синдромов $S(\bar{x})$ и $S(\bar{e}_J)$ несложно однозначно определить и сам вектор $\bar{e}$.

Таким образом, норменный метод систематизирует поиск в цепочке синдром – ошибка, да и существенно сокращает этот поиск, поскольку мощность множества ΓK $\Gamma-$орбит декодируемой совокупности K в n раз меньше мощности множества K.

Модифицированный норменный метод коррекции ошибок

Следует заметить, что с ростом n, а также с увеличением кратности корректируемых ошибок существенно увеличивается мощность $|\Gamma K|$, что сказывается на сложности декодера и скорости его работы. О сказанном свидетельствует следующая табл.1.

Таблица 1. **Количество ошибок и Г-орбит ошибок весом 2 – 4 на различных длинах**

Размерность n		7	15	31	63	127	255
Ошибки весом 2. Количество	ошибок	21	105	465	1953	8001	32385
	Г-орбит	3	7	15	31	63	127
Ошибки весом 3. Количество	ошибок	35	455	4495	39711	333375	2731135
	Г-орбит	5	31	145	631	2625	10711
	В т.ч. неполных	-	1	-	1	-	1
Ошибки весом 4. Количество	ошибок	35	1365	14465	595665	10334625	182061175
	Г-орбит	5	91	1015	9455	81375	674751

Следующая табл. 2 демонстрирует, что удельный вес векторов-ошибок с нулевой первой компонентой синдрома относительно невелик.

Таблица 2. **Количество T_ω векторов ошибок с $s_1 = 0$ весом $\omega = 3,4,5$ в двоичных БЧХ-кодах длиной $n = 7 \div 255$ а так же количество ΓT_3 – Г-орбит этих векторов**

T_ω и ΓT_ω	Длина БЧХ-кода n					
	7	15	31	63	127	255
T_3	7	35	155	651	2667	10795
ΓT_3	1	3	5	11	21	43
T_4	7	105	1085	39060	82677	680085
ΓT_4	1	7	35	620	651	2667
T_5	0	168	5208	103509	330708	33732216
ΓT_5	0	12	168	1643	2604	132284

Ниже рассматривается модификация норменного метода коррекции ошибок. В её основе лежит преобразование декодируемых ошибок, синдромы которых имеют ненулевую первую компоненту, в векторы ошибок с $s_1 \neq 0$.

Продемонстрируем модификацию норменного метода на наиболее обширном и важном для приложений классе БЧХ-кодов C_t с проверочной матрицей $H = (\beta^i, \beta^{3i}, ..., \beta^{(2t-1)i})^T$, исправляющих $t-$кратные ошибки [1 – 3]. Здесь длина n кода C_t нечётна, делит число $2^m - 1$ для некоторого наименьшего натурального $m > 1$, а $\beta -$элемент порядка n мультипликативной группы поля Галуа $GF(2^m)$.

Пусть ТКС с кодом C_t приняла вектор-сообщение $\bar{x} = \bar{c} + \bar{e}$ с неизвестным вектором-ошибкой $\bar{e}$, но с известным синдромом $S(\bar{x}) = H \cdot \bar{x}^T = (s_1, s_2, ..., s_t)$ и предположительно, с весом t. Здесь $\bar{c} -$истинное сообщение. Пусть $x_1, x_2, ..., x_t -$локаторы ошибочных позиций принятого сообщения $\bar{x}$. Это элементы первой строки матрицы H как матрицы с элементами из поля $GF(2^m)$, соответствующие ошибочным позициям. Покоординатная запись векторного равенства $S = H \cdot \bar{x}^T$ приводит к следующей системе уравнений:

$$\begin{gathered} x_1 + x_2 + ... + x_t = s_1, \\ x_1^3 + x_2^3 + ... + x_t^3 = s_2, \\ \text{..... ....} \\ x_1^{2t-1} + x_2^{2t-1} + ... + x_t^{2t-1} = s_t. \end{gathered} \tag{1}$$

Предполагается, что $s_1 \neq 0$. От вектора-ошибки $\bar{e}$ перейдём к вектору $\bar{e}^*$ с локаторами ошибочных позиций

$$x_1^* = x_1 + s_1, \; x_2^* = x_2 + s_1, ..., \; x_t^* = x_n + s_1. \tag{2}$$

Система (1) для локаторов ненулевых координат вектора $\bar{e}^*$ преобразуется следующим образом.

$$x_1^* + x_2^* + ... + x_t^* = (x_1 + s_1.) + (x_2 + s_1) + ... + (x_t + s_1) = (t+1)s_1 = 0;$$

С учётом формулы $(a+b)^{2\tau+1} = (a^{2\tau} + b^{2\tau})(a+b) = a^{2\tau+1} + a^{2\tau}b + ab^{2\tau} + b^{2\tau+1}$ имеем

$$x_1^{*3} + x_2^{*3} + ... + x_t^{*3} = (x_1 + s_1.)^3 + (x_2 + s_1)^3 + ... + (x_t + s_1)^3 =$$

$$= (x_1^3 + x_2^3 + ... + x_t^3) + s_1(x_1 + x_2 + ... + x_t)^2 + s_1^2(x_1 + x_2 + ... + x_t) + ts_1^3 = s_2 + (t+2)s_1^3 = s_2 + s_1^3.$$

Аналогичные вычисления показывают, что

$x_1^{*5} + x_2^{*5} + ... + x_t^{*5} = (x_1 + s_1.)^5 + (x_2 + s_1)^5 + ... + (x_t + s_1)^5 = s_3 + s_1^5$; и так далее

$$x_1^{*(2t-1)} + x_2^{*(2t-1)} + ... + x_t^{*(2t-1)} = (x_1 + s_1.)^{2t-1} + (x_2 + s_1)^{2t-1} + ... + (x_t + s_1)^{2t-1} = s_t + s_1^{2t-1}.$$

Таким образом, из (1) получим следующую систему уравнений:

$$\begin{gathered} x_1^* + x_2^* + ... + x_t^* = 0, \\ x_1^{*3} + x_2^{*3} + ... + x_t^{*3} = s_2 + s_1^3, \\ \text{..... ....} \\ x_1^{*(2t-1)} + x_2^{*(2t-1)} + ... + x_t^{*(2t-1)} = s_t + s_1^{2t-1}. \end{gathered} \tag{3}$$

Как видим, в равенствах (3) первая компонента синдрома $S(\bar{e}^*) = (s_1^*, s_2^*, ..., s_t^*)$ равна нулю. Тогда у нормы синдрома $\overline{N} = \overline{N}(S(\bar{e}^*))$ первые $t-1$ координат принимают вырожденные значения ∞ или –. Совокупность ΓK имеет относительно немного $\Gamma -$орбит с такими координатами. Об этом свидетельствуют и данные табл. 2. Следовательно, процедура определения вектора ошибок $\bar{e}^*$, а с ним и вектора $\bar{e}$, легко реализуется норменным методом.

Пример 1. Пусть ТКС функционирует на основе БЧХ-кода C_7 длиной 31 с проверочной матрицей $H = (\alpha^i, \alpha^{3i}, \alpha^{5i})^T$ для примитивного элемента α поля $GF(2^5)$, корня полинома $x^5 + x^4 + x^2 + x + 1$. Пусть приёмное устройство ТКС приняло сообщение с синдромом ошибок $S = (\alpha^{28}, \alpha^{29}, \alpha^{28})$. В этом случае система (1) имеет вид:

$$\begin{cases} x_1 + x_2 + x_3 = \alpha^{28}, \\ x_1^3 + x_2^3 + x_3^3 = \alpha^{29}, \\ x_1^5 + x_2^5 + x_3^5 = \alpha^{28}. \end{cases} \quad (4)$$

Сделаем в (4) замену $x_1 = x_1^* + \alpha^{28}$, $x_2 = x_2^* + \alpha^{28}, ..., x_t = x_t^* + \alpha^{28}$. Получим

$$\begin{cases} x_1^* + x_2^* + x_3^* = 0, \\ x_1^{*3} + x_2^{*3} + x_3^{*3} = \alpha^{24}, \\ x_1^{*5} + x_2^{*5} + x_3^{*5} = \alpha^{29}. \end{cases}$$

Как известно [1, 2], в коде C_7 норма синдрома $\bar{N} = (N_1, N_2, N_3)$, где $N_1 = s_2 / s_1^3$; $N_2 = s_3 / s_1^5$; $N_3 = s_3^3 / s_2^5$. Тогда $\bar{N}^* = \bar{N}(S(\bar{e}^*)) = (\infty, \infty, \alpha^{29})$. Табл. 2 указывает на наличие в данном БЧХ-коде C_7 лишь пяти Г-орбит тройных векторов-ошибок с $s_1 = 0$. В табл. 3 приведен весь список этих Г-орбит.

Таблица 3. **Образующие Г-орбит тройных ошибок, их синдромы и нормы синдромов в (31, 16) – БЧХ-коде C_7 с нормой вида $\bar{N} = (\infty, \infty, \beta)$**

№ п/п	Образующая $\bar{e}_i$	Синдром $S(\bar{e}_i)$	Норма $\bar{N}_i = \bar{N}(S(\bar{e}))_i$
1	$(1, 2, 20)$	$(0, \alpha^{20}, \alpha^{12})$	$(\infty, \infty, \alpha^{29})$
2	$(1, 3, 8)$	$(0, \alpha^{9}, \alpha^{24})$	$(\infty, \infty, \alpha^{27})$
3	$(1, 5, 15)$	$(0, \alpha^{18}, \alpha^{17})$	$(\infty, \infty, \alpha^{23})$
4	$(1, 4, 12)$	$(0, \alpha^{14}, \alpha^{18})$	$(\infty, \infty, \alpha^{15})$
5	$(1, 10, 16)$	$(0, \alpha^{24}, \alpha^{19})$	$(\infty, \infty, \alpha^{30})$

Из табл. 3 следует, что вектор $\bar{e}^*$ принадлежит Г-орбите J, порождённой вектором $\bar{e}_{орб} = (1, 2, 20)$ – с ненулевыми координатами на первой, второй и 20-й позициях. Осталось определить величину циклического сдвига вектора $\bar{e}_{орб} = (1, 2, 20)$ для получения $\bar{e}^*$. Конкретное значение этой величины получается сравнением синдромов $S(\bar{e}_{орб}) = (0, \alpha^{20}, \alpha^{12})$ и $S(\bar{e}^*) = (0, \alpha^{24}, \alpha^{29})$. Если в БЧХ-коде C_7 синдром $S(\bar{e}) = (s_1, s_2, ..., s_t)$, то синдром $S(\sigma(\bar{e})) = (\alpha \cdot s_1, \alpha^3 \cdot s_2, ..., \alpha^{2t-1} \cdot s_t)$ [4 –5].

Существует такое натуральное k, что $\sigma^k(\bar{e}_{орб}) = \bar{e}^*$. Следовательно, $20 + 3k = 24 + 31l$ для подходящего целого l или $3k = 4 + 31l$. Подберём наименьшее l, при котором $31l + 4$ делится на 3. Легко видеть, что требуемое $l = 2$. Тогда $31l + 4 = 66 = 3 \cdot 22$, то есть $k = 22$. Следовательно, $\bar{e}^* = (11, 23, 24)$. Поэтому $x_1^* = \alpha^{10}$, $x_2^* = \alpha^{22}$, $x_3^* = \alpha^{23}$. Тогда

$x_1 = x_1^* + \alpha^{28} = \alpha^{10} + \alpha^{28} = \alpha^9$, $x_2 = x_2^* + \alpha^{28} = \alpha^{22} + \alpha^{28} = \alpha^{13}$, $x_3 = x_3^* + \alpha^{28} = \alpha^{23} + \alpha^{28} = \alpha^{21}$.

Вычисленные локаторы однозначно высвечивают искомую вектор-ошибку $\bar{e} = (10, 14, 22)$.

Замечание. *Отметим, что рассмотренное преобразование локаторов (2) допустимо только при выполнении одного трудно проверяемого условия: ни один из локаторов* x_i *ненулевых координат искомого вектора-ошибки* $\bar{e}$ *не должен совпадать с* s_1. *Дело в том, что тогда* $x_i^* = 0,$ *а таких локаторов проверочная матрица БЧХ-кода* C_t, *очевидно, не имеет. Для тройных ошибок названное требование выполняется: если бы, скажем,* $s_1 = x_1 + x_2 + x_3 = x_1,$ *то тогда* $x_2 + x_3 = 0,$ *то есть* $x_3 = x_2,$ *что невозможно – локаторы координат векторов попарно различны.*

Заключение

Разработана модификация норменного метода коррекции ошибок. Реализуется путём отображения этих ошибок в ошибки того же веса, но с первой компонентой синдрома, равной нулю. Спектр таких ошибок небольшой по сравнению с их общим количество. Это существенно ускоряет работу декодера. Особенно эффективен метод при коррекции кодами трёхкратных ошибок.

NORM DECODING OF ERRORS VIA THEIR MODIFICATIONS

V.A. LIPNITSKI, E.K. AL-HAIDAR

Abstract

Modified norm decoding method of errors in binary BCH random length and random distance codes had been proposed. The essence of this method is in mapping errors with the first nonzero syndrome component in the error with the same weight where the first syndrome component is equal to zero.

Литература

1. *Мак-Вильямс, Ф.Дж.* // Теория кодов, исправляющих ошибки. М., 1979.
2. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. М., 1986.
3. *Конопелько, В.К., Липницкий, В.Д. Дворников и др*. Теория прикладного кодирования: Учебное пособие. М., 2004.
4. *Конопелько, В.К., Липницкий В.А*. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. М., 2000.
5. *Липницкий В.А*. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. М., 2007
6. *Курилович А.В., Липницкий В.А., Аль-Хайдар Е.К. //* Докл. БГУИР. 2005, №6. 28 – 30.